Iain Dickson
@wan0net@infosec.exchange

So you want to build a Security Operations Capability?

What will I be covering?

- What is a security operations capability?
- What is the most important question to start with?
- What do you do after you've answered the question?
- What are some real gotchas that you really need to pay heed to?

What the hell do I know about SOCs?

- 10 years in Cyber Security, 13 (inclusive) in IT

- Previous Positions
  - Cyber Security Research Engineer at AU DOD
  - Assistant Director Cyber Threat Intelligence Technical Capability at AU DOD
  - Security Operations Centre Lead at Leidos Australia
  - Chief Cyber Architect at Leidos Australia

- Currently the Cyber Practice Lead for Leidos Australia, reporting up to the CTO.

- Founder for ComfyConAU

What is a security operations capability?

A security operations center (SOC) is a **centralized unit** that deals with security issues on an **organizational** and **technical** level. It comprises the three building blocks **people**, **processes**, and **technology** for managing and **enhancing an organization's security posture**.

A SOC can include:

- Monitoring and Incident Response
- Threat Intelligence
- Governance Risk and Compliance
- Engineering and Architecture
- Vulnerability Management
- Penetration Testing
- ITSM

The composition of your SOC is driven by the organisational requirements - built using lego bricks.

What is the most important question to start with?

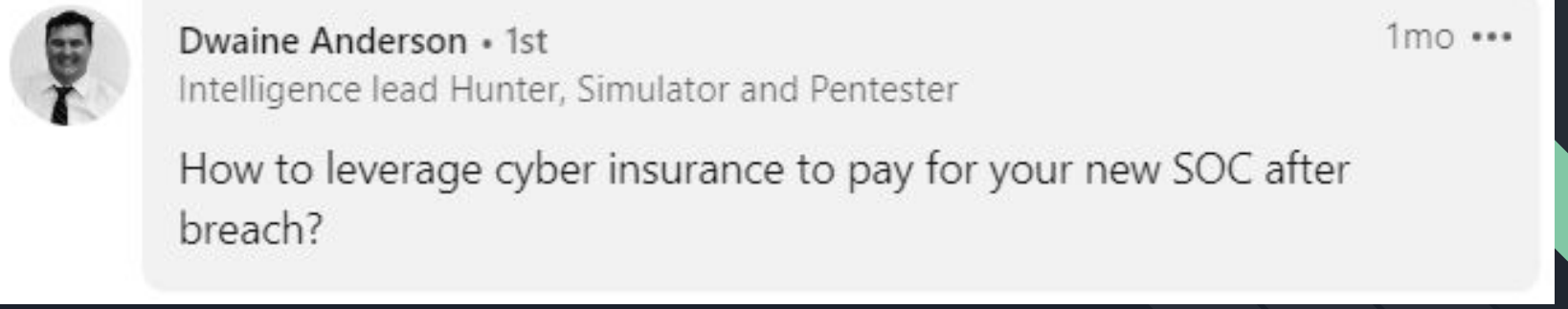
Imagine the scene...

Iain Dickson

ComfyCon AU Founder, Cyber Handyman for Leidos Australia

1mo •

My BSides talk is going to be about how to set up a successful security operations center. I'd like to know from you guys, what you think the single most important question that should be asked in the planning stage is? What is the defining question that will drive the rest of the development of the SOC?


Dwaine Anderson • 1st
Intelligence lead Hunter, Simulator and Pentester
1mo •••
How to leverage cyber insurance to pay for your new SOC after breach?

Dean Correia • 1st
Leidos Australia Business Information Security Officer
1mo •••

What business outcomes is the SOC supporting?

Frode Hommedal • 2nd
Helping businesses become defendable
1mo •••

Iain Dickson "Why?"

George Coldham (He/Him) • 1st
Cyber Security Professional | Senior Consultant at Empired Ltd
1mo •••

What do you hope to achieve, what is your vision for this, why do you need.... does this activity support the strategy of the business, do you have the resources to do this... should you outsource this...

Edward Farrell • 1st
Cyber security nerd, Director, Advisor, Industry Fellow @ UNSW Canberra
1mo •••

Same goes with any IT project for the past 50 years- identify the purpose. Cyber is nested in tech, which is nested in the businesses endstate. If you cannot identify the whats, then the SOC is little more than a white elephant which will be apparent
in your teams execution.

Mickey Perre • 1st
Cyber Security Strategist at Devo
1mo •••

Do I need a SOC? and what organisational pre-reqs help for a successful SOC. I.e you don't need a SOC if you are a two person team.

Andrew Scully • 1st
Head of Cyber Security Consulting at Ampion (formerly Shelde) | Board ...
1mo •••

Why are we building a SOC? What are you trying to achieve?

Braden Anderson • 2nd
Aligning InfoSec with business goals
1mo •••

What is the business risk the SOC will mitigate? Answering this informs the target level of capability and justifies the budget.

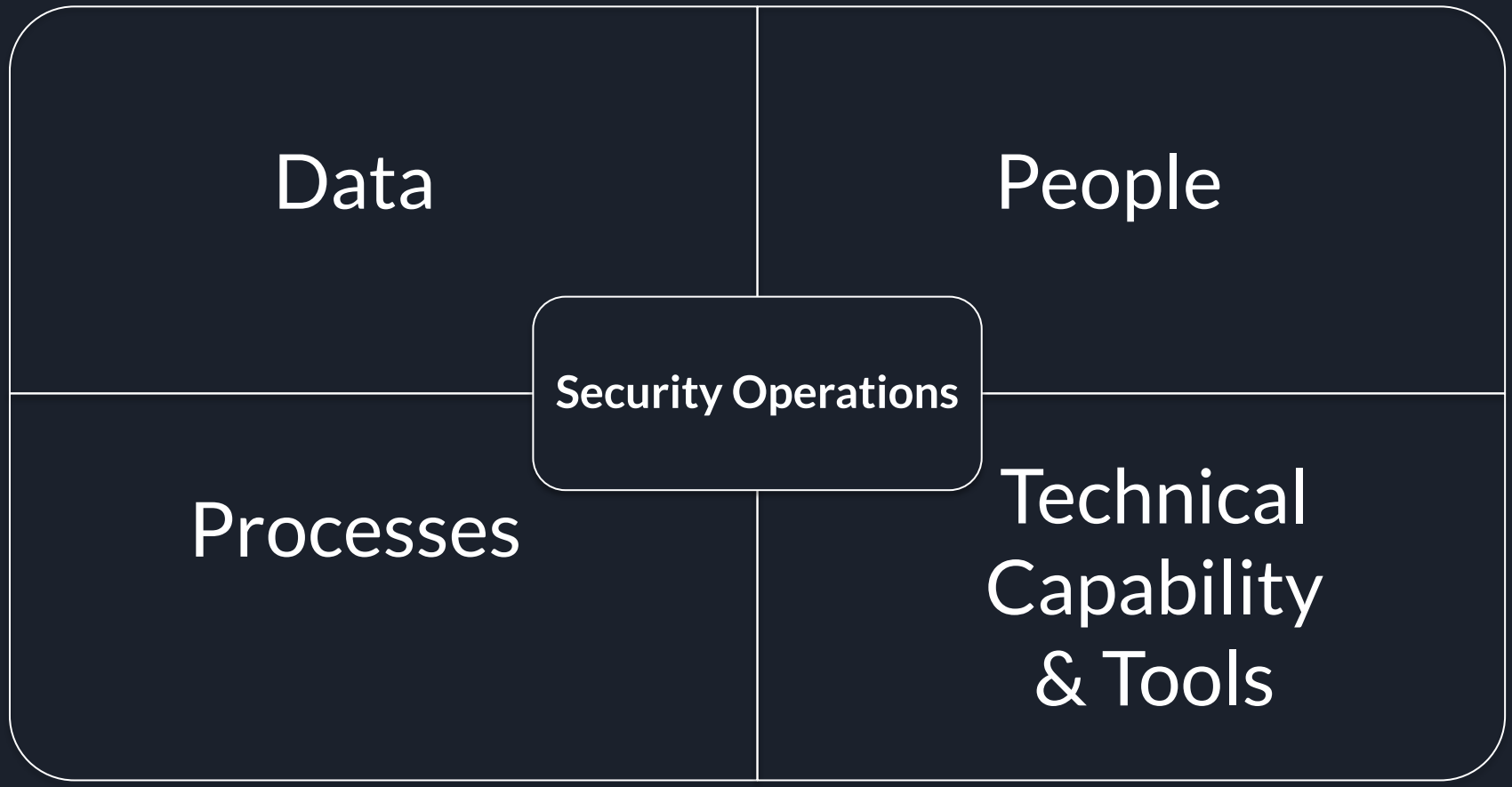

CISO
SOC
BASIC
CYBER HYGIENE
imgflip.com

Why, why, why Delilah?

- Identifying the mission purpose gives you:
  - Direction
  - Prioritisation
  - A rough idea on budget
- All of these then feed into your actual implementation of a SOC.
- Remember also: Understanding why (and having a clear understanding of what) means you can deliver on management's expectations.

What next?

Component Parts of Security Operations Capability



Threat Actor Tiers

Resources

Volume

Tier VI
Nations, Global 25

Tier V
Nations, Global 150, State Sponsored

Tier IV
Organised Crime, Cyber Mercenaries

Tier III
Crime Groups, Hacktivists

Tier II
Criminals, Disgruntled Workers. Programmers

Tier I
Script Kiddies, Non Malicious Actors

Creates Vulnerabilities using Full Spectrum

Discovers Unknown Vulnerabilities

Exploits pre-existing, known vulnerabilities

https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-081.pdf

So what are some real gotchas?

Timeframes

- Building a mature SOC will take time no matter how much money you throw at it.
- There are a number of challenges which if you're building from scratch will take time
  - Data acquisition and visibility across the enterprise
  - Development and refinement of SOP's through use "in anger"
  - Team Forming / Storming / Norming
  -
- A SOC is never finished. It is always constantly evolving in order to mitigate future threats and adapt to new technologies.
- Have a realistic timeframe, with a clear definition of done.

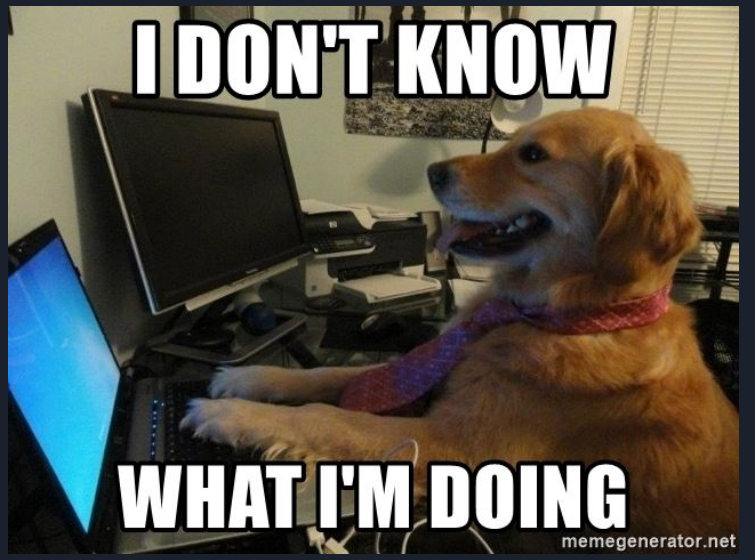
Hiring

- Your hiring location is going to be a significant factor on resourcing.
- Canberra, Sydney and Melbourne - Facing a drain at the moment.
- Also intimately linked is Security Clearance requirements - if not hiring with one, then need to factor into your timeframes.
- *Side note: Make sure you market test salaries and start off with a reasonable figure.*

Shift Rosters

- What is the expectation of the SOC?
  - 9-5 5 days a week?
  - 7-7?
  - 24 hours 7 days a week?
- The increase in manning hours can dramatically increase resourcing.
- You ideally need between 2 and 3 people for each skill set in order to ensure continuity.
- You also can't have a shift of one person, and you need backups in order to cover.
- This can blow a SOC of 10 people, out to 50.

Training!



- Don’t rely on vendor and external training. You will need to develop a comprehensive training plan that includes:
  - Internal organisational training (including onboarding)
  - External generic training
  - Specific vendor training targeted at the environment.
- Online training is becoming a great offering to team members in order to wile away those long shift hours.

SOPs

- People will leave. Things will change. Corporate knowledge is not something to be relied on.
- Make developing a _workable_ knowledge management strategy a priority
  - How should information be captured?
  - How should it be reviewed and when?
  - What should be captured?
- There is a balance between too granular, and not granular enough.
  - The use of tools such as SOAR and Automated Playbooks also supports this effort.

Metrics

- Metrics are a key way of indicating to management the success of a SOC.
- DO NOT USE INCIDENT COUNTS OR ALERT COUNTS
  - You need to develop metrics that enable decisions to be made on improvements.
  - Number of incidents and number of alerts are not really tied to any decisions that can be made.
    - Number of incidents when establishing a SOC is high, because you're finally catching stuff.
- Look at building metrics that measure elements of the process.
  - Time to Identify
  - Time to Contain
  - Machines vulnerable above the agreed baseline
- Especially important to get these right in an SLA based organisation.
- Side Note: Ensure in an ITIL / ITSM organisation that you have a separate metric/SLA for Incident vs. Security Incident.

In closing

Summary

- A SOC can be whatever you want it to be. You need to sta with clear direction from either management or a custom on what they want to be a part of the SOC.
- Understanding the business purpose is a key directional indicator for where you should develop and focus the SO
- It's an integrated model of data, people, processes and technology. Any one part of this model can bring down th entire team.
- I've had a lot of tricky situations with the areas of focus, and I hope you can learn from those.

Thanks!

icd@wan0.net
@wan0net